our energy your success

SOLVAY
asking more from chemistry®

LA GOVERNANCE DELLA CYBERSECURITY IN SOLVAY

ANTONIO GIUSTINO – IS INDUSTRIAL RISK MANAGER

MILANO,26 SETTEMBRE - 2019
AUDITORIUM FEDERCHIMICA

2018 KEY FIGURES

24,500
Employees

61
Countries

115
Industrial sites

21
Major R&I centers

TOP 3
Market position in
~ 90% of portfolio

€10.3 billion
Underlying net sales

€2.2 billion
Underlying EBITDA

Figures take in account the planned divestment of the polyamide business

50%
Net sales generated by sustainable solutions

We are an advanced materials and specialty chemicals company, committed to address key societal challenges

SOLVAY
asking more from chemistry®

Agenda

1. Industry 4.0-background
2. La minaccia cyber per l'industria e sue attuali vulnerabilità
3. *Differenze e convergenza OT-IT*
4. La governance olistica della security in Solvay
5. L'approccio per la cybersecurity in Solvay
6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

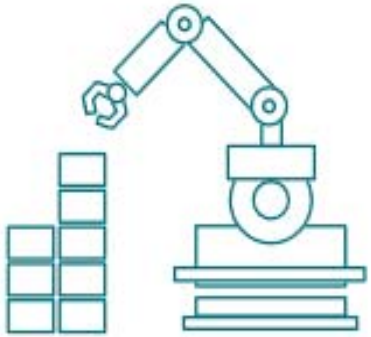
…..-> INDUSTRY 4.0

Late 18th–19th century

First Industrial revolution:
Power generation

Beginning of 20th century

Second Industrial revolution:
Industrialization



1970s–2000s

Third Industrial revolution:
Electronic automation

2010 onward

Fourth Industrial revolution:
Smart automation…and exponential change

Source: Deloitte Insights, *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*

SOLVAY
asking more from chemistry®

TRASFORMAZIONE DIGITALE IN OT (OPERATIONAL TECHNOLOGY)

SOLVAY
asking more from chemistry®

LE 9 COMPONENTI DELL' INDUSTRY 4.0

SOLVAY
asking more from chemistry®

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [1/4]

+ Profitable

+ Organized

+ Sophisticated

+ Aimed to the target

+ Frequent and Severity

-> new technologies, skills, processes are required continuously for risk mitigation ..

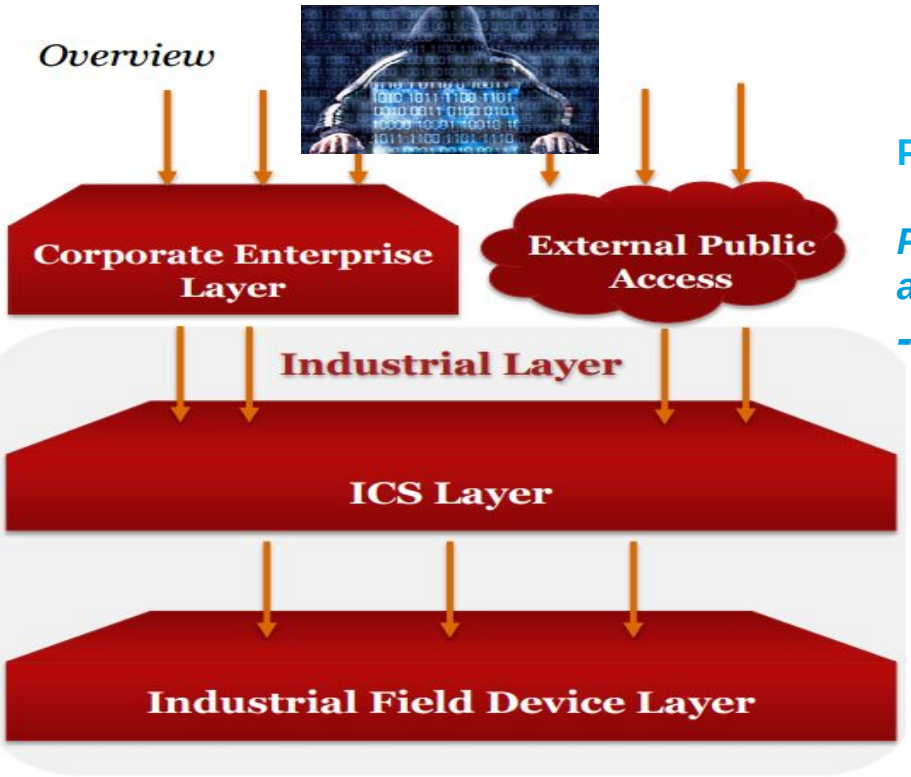
SOLVAY
asking more from chemistry®

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [2/4]

IT:
corp.*network,WEB, ERP, email ,file servers,collaboration ...*

OT :
PLC,HMI,SIS,DCS, SCADA …

Field devices (sensori,attuatori..)



Source : PWC

PRINCIPALI MINACCE:

Furto di informazioni, danni all'operatività del business,..

Danni alla produzione, agli impianti e possibili conseguenze HSE,..

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [3/4]

In ICS gli attacchi sono principalmente di tipo cyber «fisico» :

Equipment Damage

- *Equipment overstress*
- *Safety limits violation*

Production Damage

- *Product quality*
- *Production rate*
- *Operating costs*
- *Maintenance efforts*

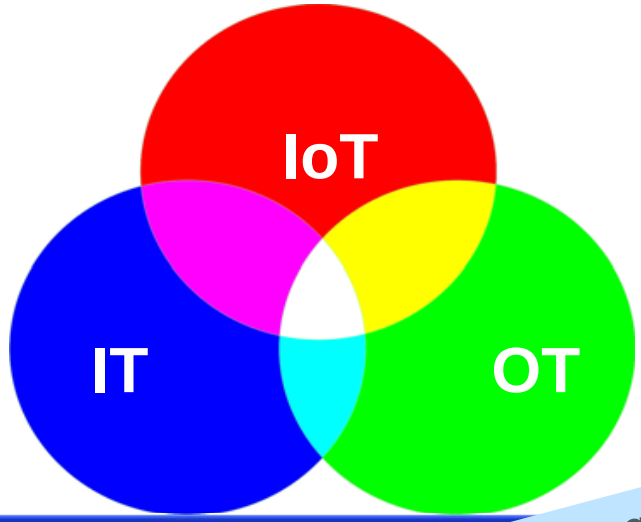
Compliance Violation

- *Safety*
- *Pollution*
- *Contractual treatles*

SOLVAY
asking more from chemistry®

LA MINACCIA *CYBER* PER L'INDUSTRIA E SUE ATTUALI VULNERABILITÀ [4/4]

IT-IoT-OT : complexity & risk are increasing …



Some new threats in progress:
- A.I. and M.L.
- Mobile devices
- Robotic and AGV
- Unsecure coding
- Multi-clouds environment
- Drones
- Digital & connection with stakeholders
-

IoT report (tbc): 2018/17:
Turnover = 40%
Declared incidents = + 280%

WHY ?

AUJAS

2 recents good news in 2019 :
- ETSI released standard for IoT security (basis for IoT certification)
- EU 'Cybersecurity ACT' regulation for certification is coming (voluntary at the moment! ..)

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

Attuali principali differenze operative IT vs OT

	IT	OT
- CICLO DI VITA	- 3-5 anni	- 10-20 anni
- RISCHIO PIU TEMUTO	- Perdita dati/info	- Vita,assets,ambiente
- SEC. PRIORITY (C.I.A.)	- Confidentialità dati	- Disponibilità sistemi
- REBOOT	- Accettato	- Non accettato
- CHANGE MANAGEMENT	- Frequente/automatico	- Raro/accurato
- SISTEMI	- Standard	- Prorietari
- TEMPI DI RISPOSTA	- Ammesso ritardo	- Real time
- COMUNICAZIONE..	- Protocolli std	- Protocolli prop. + std

SOLVAY
asking more from chemistry®

La convergenza IT-OT è un inevitabile processo per supportare la trasformazione digitale : qualche nostro suggerimento per favorire la cooperazione a regime ..

@ IT & OT :

. Comprendere il cyber risk “tollerato” definito dalla strategia aziendale
. Definire e condividere le politiche di cybersecurity e le architetture
. Concordare gli obiettivi/priorità/piano operativo comune
. Condividere/prevenire gli impatti reciproci delle attività
. Rendere visibili tutte le componenti in gioco e verificare le competenze
. Lavorare per processo rispettando ruoli/responsabilità
. Dotarsi di tools adeguati ad uso trasversale (monitoraggio,work-flow,..)
. Definire regole di controllo, intercettazione anomalie ed azioni conseguenti di tipo tecnico ed organizzativo (SOC,SIEM,UEBA,Sonde OT, IRP,..)
. Simulare scenari di crisi e relativa escalation,..

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

LA GOVERNANCE OLISTICA DELLA SECURITY IN SOLVAY

Solvay Responsible Care policy commits us to ensure adequate protection of people, property, products, plants, transport, information and information systems against security threats: criminal, malicious and cyber acts.

policy commits us to ensure adequate
, property, products, plants, transport,
d information systems against security threats:
, malicious and cyber acts.

Solvay's Security Code

Our Security Code defines the management principles that we strive to implement to continuously enhance security using a threat- and risk-based approach to identify, to assess and address vulnerabilities, to enhance response capabilities and to maintain and improve relationships with key stakeholders.

1. Leadership Commitment.
Solvay leadership commits to continuous security improvement through published policies, provision of sufficient and qualified resources and established accountability.

2. Analysis of Threats, Vulnerabilities and Consequences.
Potential security threats, vulnerabilities and consequences are to be prioritized against accepted criteria and regularly analyzed.

3. Implementation of Security Measures.
Security measures are to be developed and implemented commensurate with risks, and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.

4. Information and Cyber-Security.
Protecting information and information systems is recognized as a critical component of a sound security management system, and security measures are developed and implemented accordingly.

5. Documentation.
Security management programs, processes and procedures are to be documented.

6. Training, Drills and Guidance.
As appropriate, training, drills and guidance are to be provided for employees, contractors, service providers, value chain partners and others, to enhance awareness and capability.

7. Communications, Dialogue and Information Exchange.
Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies is to be maintained, balanced with safeguards for sensitive information.

8. Response to Security Threats.
Security threats are to be evaluated and responded to and reporting and communication of security threats is to be performed as appropriate.

9. Response to Security Incidents.
Significant security incidents are to be evaluated, responded to, investigated, communicated as appropriate, reported to the Group, and corrective action to mitigate impact and reoccurrence implemented.

10. Audits.
Periodically, our security programs and processes and implementation of corrective actions are to be audited. This may include third-party verification where required.

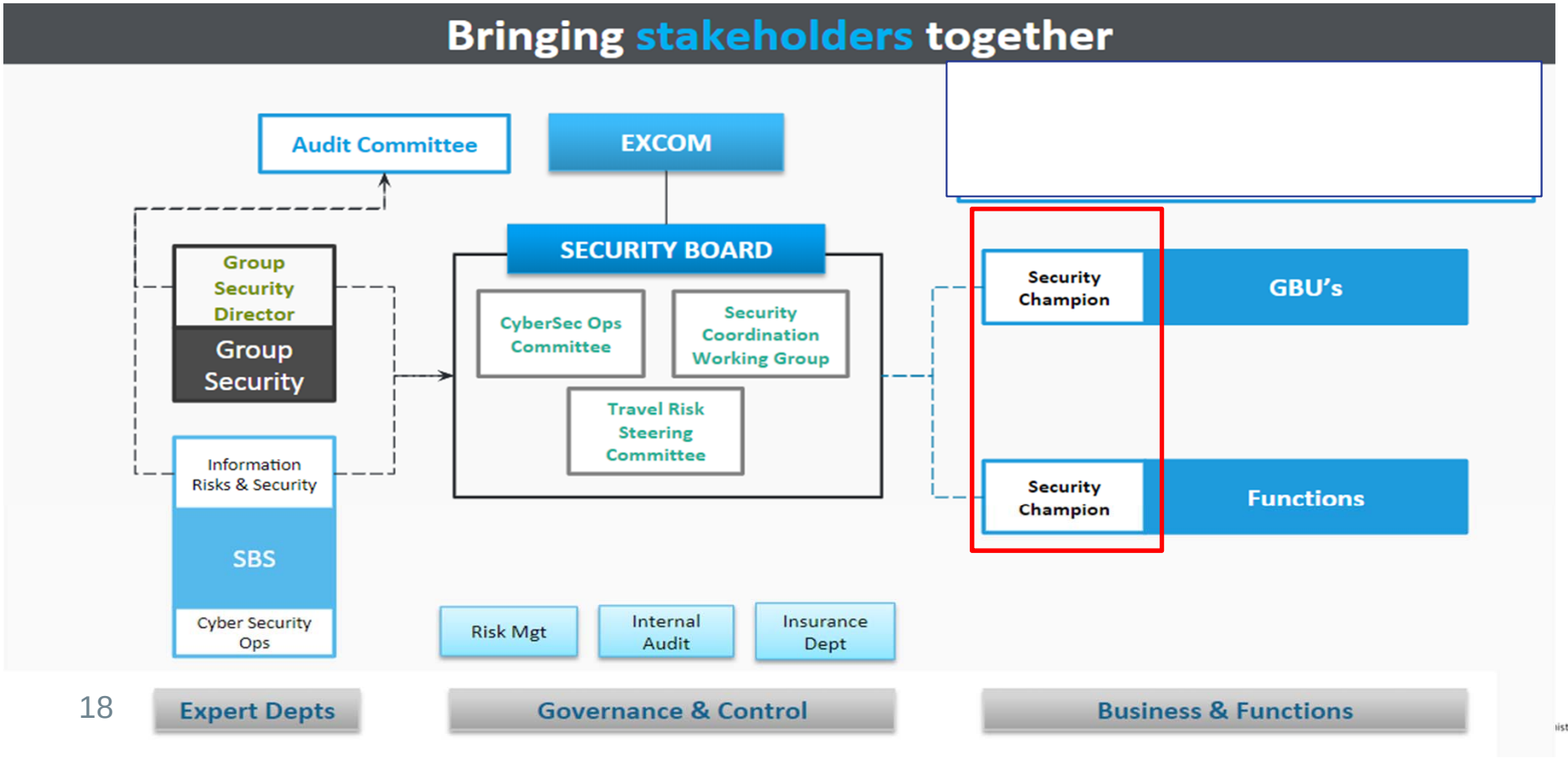
11. Management of Change.
Changes involving people, property, products, processes, information or information systems are to be evaluated for security risks, which are to be properly managed if identified.

12. Continuous Improvement.
Continuous improvement processes are to be established entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.

SOLVAY

SOLVAY
asking more from chemistry®

L’ organizzazione della Governance olistica per la Security



Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

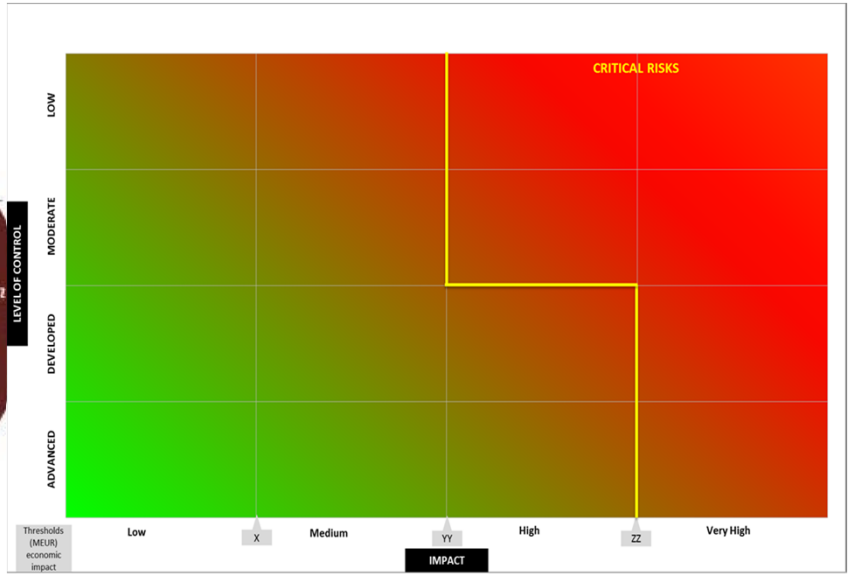
4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

L’ approccio per la cyber security in Solvay : RISK

Source : PwC




1

CORPORATE GOVERNANCE

This chapter is an annex to the management report

MANAGEMENT OF RISKS 59

1 Main risks 60

Innovation failure 60

Transport accident 61

Information protection and cyber risk 61

Ethics and compliance 61

Chemical product usage 62

Projects selection and management 62

5 types of impact

Economic

Injury to people

Reputation

Environment

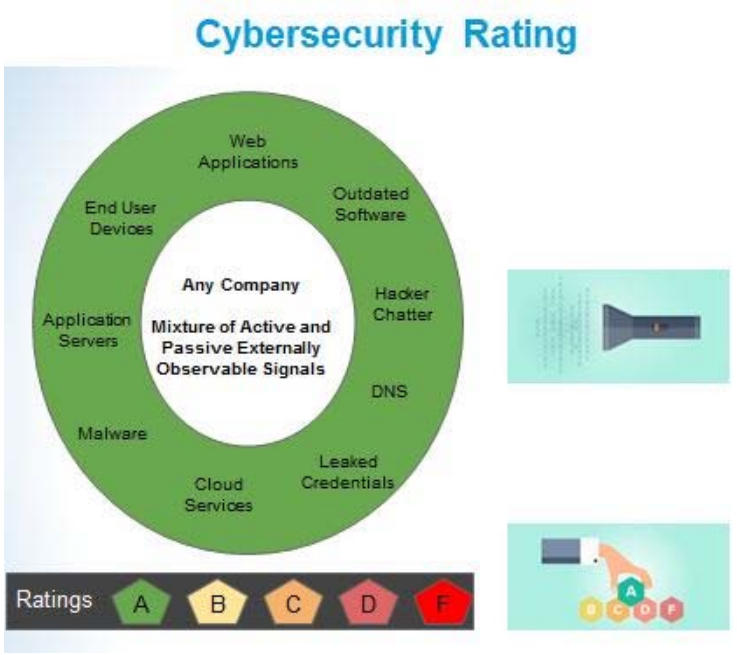
Legal

Information prot

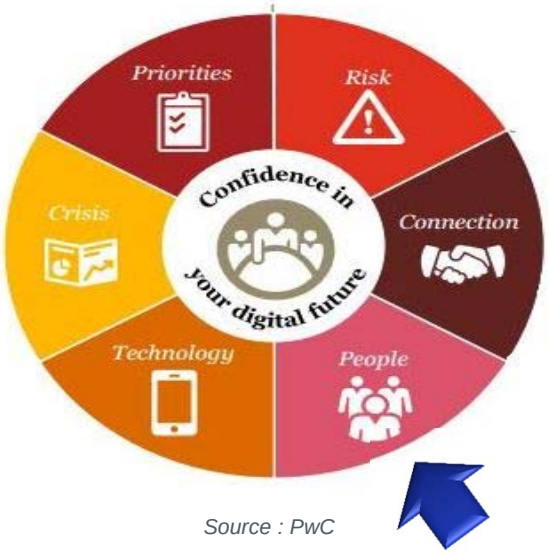
SOLVAY
asking more from chemistry®

L’ approccio per la cyber security in Solvay : CONNECTION

Source : PwC



L’ approccio per la cyber security in Solvay: PEOPLE



Source : PwC

--- Questo messaggio è destinato all'utente Antonio-Michele Giustino ---

Buongiorno,

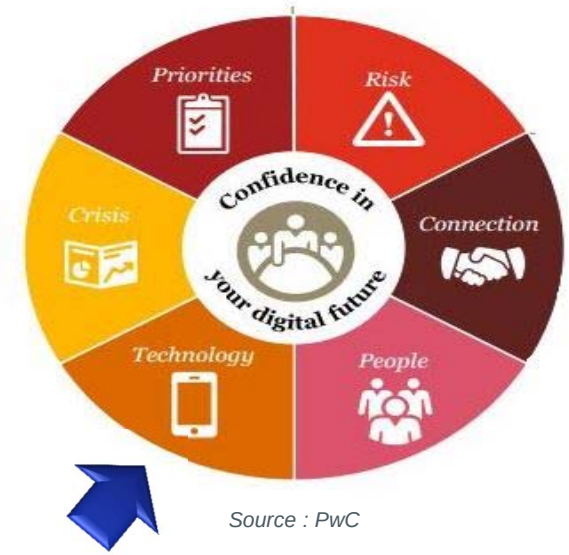
le ricordiamo che la formazione online training "Certificazione eSecurity" è obbligatoria per tutti i collaboratori di SOLVAY che abbiano accesso alla rete aziendale.
Ha ricevuto questo messaggio perché il certificato conseguito scadrà tra 1 settimana.
Senza certificazione, il suo accesso a Internet potrebbe essere sospeso 4 settimane dopo la data di ricezione del presente messaggio. L'accesso sarà riattivato non appena avrà conseguito la certificazione.

Per accedere al programma di certificazione, è sufficiente fare clic sul link sguente: Fare clic qui.

Grazie per la partecipazione e per il contributo attivo alla sicurezza dei sistemi informativi di SOLVAY.

SOLVAY
asking more from chemistry®

L’ approccio per la cyber security in Solvay: TECHNOLOGY



Source : PwC

Intelligent Detection Platform

Intelligent detection platform that continuously monitors every layer of the internet (data leak, hackers communication, sensitive code share, connected storage)


Surface Web

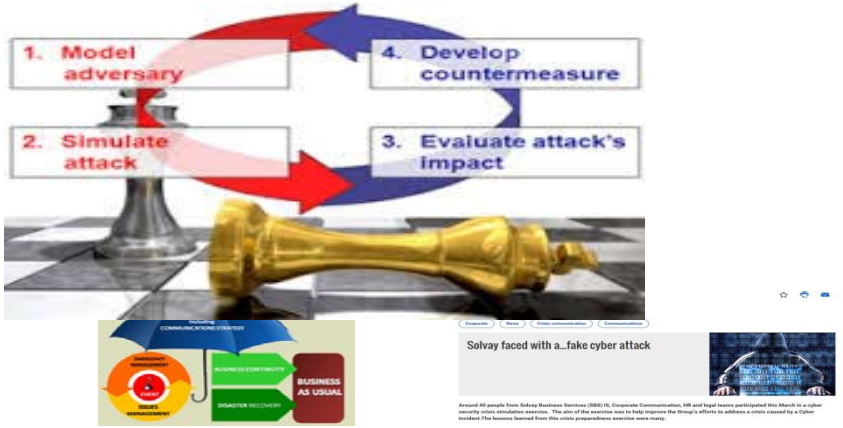

Deep Web & Dark Web


Connected Storage

SOLVAY
asking more from chemistry®

L’ approccio per la cyber security in Solvay: CRISIS

Source : PwC



SOLVAY
asking more from chemistry®

L’ approccio per la cyber security in Solvay: PRIORITIES

Source : PwC

SOLVAY
asking more from chemistry®

L’ approccio per la cyber security in Solvay: REPORT FINALE

Source : PwC

1 Main risks

The Group Risk Committee has assessed Group risks' impact and level of control. Four main types of impact were used: economic impact, impact on people, impact on environment and impact on reputation.

The level of control of the risks was assessed by considering the following questions:

- are the mitigating/controlling actions defined?
- are the actions implemented, fully or partially?
- is the effectiveness of those actions monitored?

Each of these criteria has been rated on a four level scale.

The criticality refers to the combination of both ratings (impact and level of control) of the risk at the time of the assessment.

In the chart hereafter, the trend reflects the evolution of criticality, taking into account the implementation of mitigating actions in 2015.

Criticality	Risk	Trend
High	Innovation failure	↘
	Transport accident	→
	Information protection and cyber-risk	↘

Information protection and cyber risk ↘

SOLVAY
asking more from chemistry®

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica della security in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il framework nazionale per la cybersecurity, privacy (GDPR) e protezione dei dati

FRAMEWORK NAZIONALE PER LA CYBERSECURITY , PRIVACY (GDPR) E DATA PROTECTION

WWW.CYBERSECURITYFRAMEWORK.IT (CIS,CINI) :

- *Ispirato dal NIST (National Institute of Standard and Technology – USA)*
- *Presentato nel 2015 nella sua forma globale*
- *Realizzata la versione ridotta per micro e PMI nel 2016*
- *Nuova versione comprensiva della privacy (GDPR) e della protezione dei dati aggiornata a febbraio 2019*
- *Possibilità di :*
  - *fare una stima dei costi per implementare le best practices essenziali (micro e PMI imprese)*
  - *fare un'autovalutazione per conoscere l'esposizione al rischio Cyber della propria realtà*
  - *individuare un target aziendale ed il conseguente percorso migliorativo di Cybersecurity.*

Grazie
per l'attenzione

SOLVAY
asking more from chemistry®

www.solvay.com

FOLLOW US ON